Stichting Pensioenfonds Thales Nederland

Beleidsnotitie ICT, informatievoorziening en cybersecurity

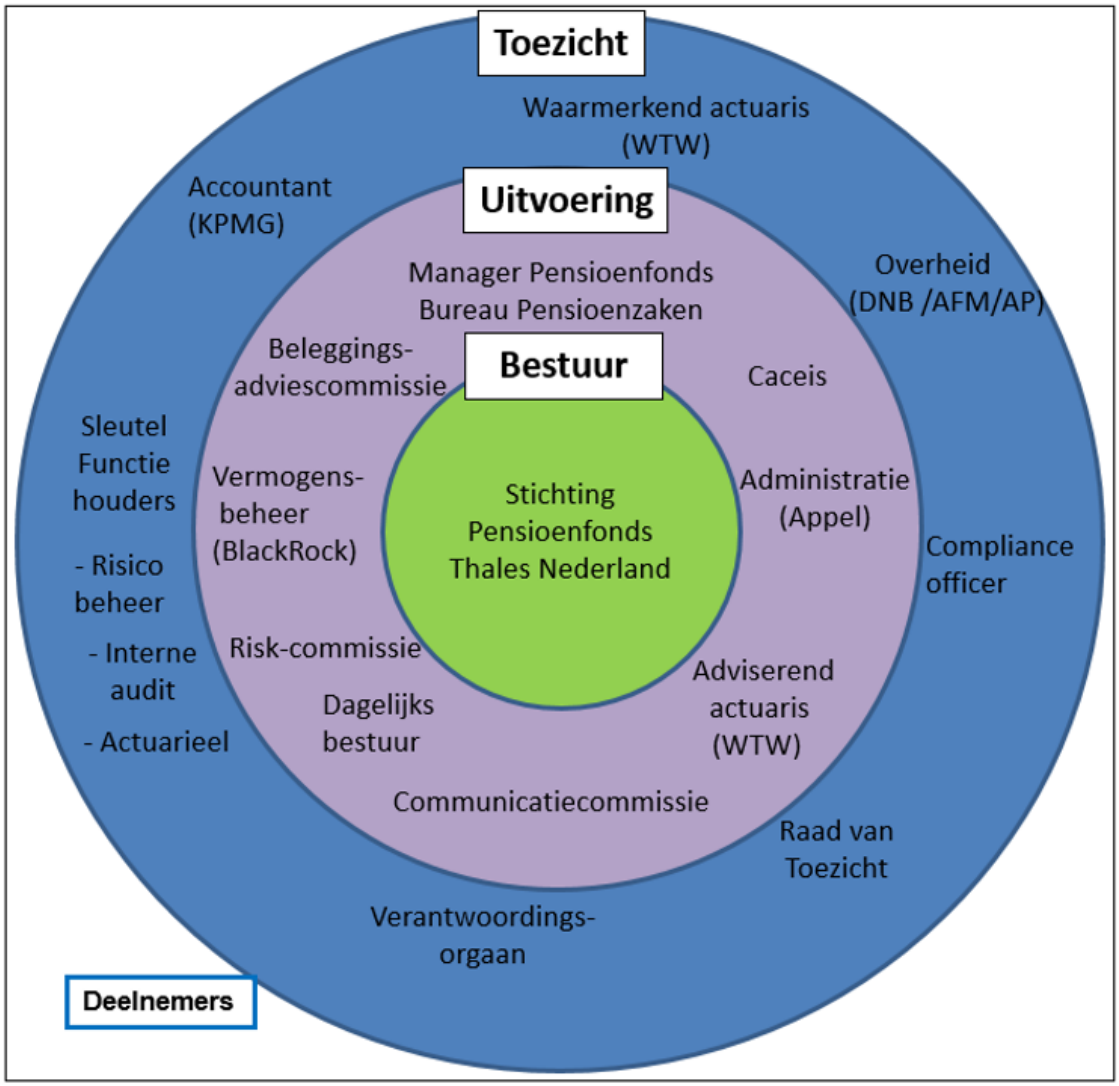
2023-2025

Inhoudsopgave

1. Management Summary

De doelstelling van het ICT- en Informatievoorzieningsbeleid is het handhaven van de beschikbaarheid, integriteit en vertrouwelijkheid (met inbegrip van authenticiteit, toerekenbaarheid en controleerbaarheid) van informatie. Het beleid van het fonds en de wijze waarop het zijn beleid auditeert is getoetst aan de meest recente richtlijnen van DNB[1], de Pensioenfederatie en de Algemene Verordening Gegevensbescherming (hierna: AVG). Naast het beleid wordt in deze notitie de huidige ICT-inrichting van het fonds beschreven. Ook wordt ingegaan op de gestelde eisen aan de ICT- en informatievoorziening en de wijze waarop deze eisen worden gerealiseerd. De looptijd van het ICT- en informatievoorzieningsbeleid is 3 jaar, 2023 tot en met 2025. Doorlopende verbetering van het ICT- en informatievoorzieningsbeleid heeft de aandacht van het bestuur.

2. Overzicht van de betrokken partijen bij het fonds



[1] - https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf
- https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2023/transitienieuws-benchmarkrapportage-informatiebeveiliging-2022/

3. ICT-toepassingen van de betrokken partijen bij het fonds
Het fonds zelf heeft geen specifieke ICT-toepassingen in eigen beheer. Alle ICT-toepassingen zijn uitbesteed aan of maken onderdeel uit van de onderstaande vijf hoofd (uitvoerings-) partijen.

1. *Thales Nederland B.V.*
Het fonds heeft een eigen website die via Thales Nederland wordt gehost. De bestuursleden en de medewerkers van Bureau Pensioenzaken maken gebruik van de ICT-omgeving zoals de firma deze ter beschikking heeft gesteld aan haar medewerkers.

2. *Appel Pensioenuitvoering*
Deze organisatie verzorgt de pensioenadministratie en pensioencommunicatie.

3. *BlackRock*
Deze organisatie verzorgt het vermogensbeheer, voert de renteafdekking uit middels een LDI portefeuille en ondersteunt het vermogensbeheer met strategische advisering.

4. *Caceis*
Deze organisatie verzorgt de administratie van beleggingen ter toetsing van de vermogensbeheerder, regelt bewaarneming, verzorgt de geconsolideerde vermogens- en verplichtingenrapportage, verzorgt de performance- en compliance meting en verzorgt een deel van de rapportage aan de toezichthouder.

5. Willis Towers Watson
Deze organisatie verricht voorkomende werkzaamheden uit hoofde van haar rol als adviserend actuaris en certificerend actuaris.

4. De strategie van het fonds
De strategie van het fonds, voortkomend uit de missie en visie van het fonds luidt: SPTN zet in op continuïteit. Het bestuur heeft continue aandacht voor de communicatie en dialoog met alle deelnemers, evenals het beleggingsbeleid en de resultaten daarvan. Hiervoor heeft het een communicatie-, een integraal risicomanagement- en een beleggingsadviescommissie ingesteld, evenals een dagelijks bestuur. De effectiviteit van het beleid wordt voortdurend gemonitord en bekeken door het bestuur, in samenwerking met het verantwoordingsorgaan en de Raad van Toezicht.

5. Algemene beschrijving van het auditeringsproces van de uitbestede ICT
Bij het fonds zijn een aantal partijen betrokken zoals hiervoor weergegeven. De uitvoeringspartijen in “de tweede schil om het fonds” hebben te maken met ICT- en informatievoorziening. Op deze partijen wordt toezicht gehouden door de toezichthouders in “de derde schil om het fonds”. Het voortdurend beheersproces van de ICT-toepassingen en informatievoorzieningen ”loopt door de schillen” van bestuur, naar uitvoering en vervolgens naar toezicht en weer terug.

Het primaire proces van het fonds heeft betrekking op de uitvoering van de pensioenregeling en het vermogensbeheer. Het primaire proces wordt vormgegeven door onder andere de administratieve organisatie rondom dit primaire proces. Dit gaat kortgezegd over wie wat doet en hoe de functiescheiding geregeld is. ICT- en informatievoorziening dient de uitvoering van het primaire proces en de administratieve organisatie te ondersteunen. In deze beleidsnotitie wordt door het fonds weergegeven aan welke eisen de ICT-toepassingen en dataverwerking in het primaire proces moeten voldoen. Vervolgens geeft het fonds weer hoe zij monitort dat de uitvoeringspartijen die ICT-toepassingen gebruiken en data verwerken voor het fonds aan deze gestelde eisen voldoen.

Dat doet het fonds door de gestelde ICT-eisen specifiek en meetbaar te maken, deze contractueel overeen te komen en op te nemen in de uitbestedingsovereenkomst per uitbestedingspartij. Aanvullend kunnen in service level agreement ‘s (hierna: SLA ‘s) nadere afspraken gemaakt worden over de contractueel overeengekomen dienstverlening. Daarnaast zullen relevante processen en de daarbij gestelde eisen zoveel mogelijk binnen de scope van audits door onafhankelijke accountants gebracht worden (zoals bijvoorbeeld ISAE 3402en/of ISAE 3000audits). Op deze wijze kan een effectieve control bewerkstelligd worden. Als het bestuur dat wenselijk acht kunnen steekproeven worden gedaan of de SLA’s goed genoeg werken. De input voor de SLA’s bestaat uit generiek gestelde eisen voor de gehanteerde tools en specifiek gestelde eisen voor de inhoud per uitvoeringspartij. In het navolgende gaat het fonds in op de gestelde eisen.

6. De zes ICT-beheers eisen

Algemeen geformuleerd verlangt het fonds voor de uitvoering van het primaire proces een betrouwbare, efficiënte en flexibele informatievoorziening waarbij de operationele stabiliteit continu geborgd is, waarbij wordt voldaan aan wet- en regelgeving en waarbij aan de hand van de geïnventariseerde en geanalyseerde ICT-risico’s deze risico’s zoveel mogelijk prioriteitsafhankelijk gemitigeerd worden.

De zes beheers eisen aan ICT- en informatievoorziening die zoals gesteld contractueel en nader vastgelegd kunnen worden in SLA’s per uitvoeringsorganisatie staan hieronder opgesomd. Daarbij moet ook rekening worden gehouden met de vier grootste ICT-risico’s welke daarna worden opgesomd.

1. Kantoorautomatisering bij de uitvoeringspartijen
    - De ICT-toepassingen en data verwerking bij de uitvoeringspartijen en de administratie en organisatie moet zodanig worden ingericht dat aan de verlangde eisen aan data hierna onder punt 2 tot en met 5 wordt voldaan.
2. Deelnemersdata
    - De deelnemersdata dient juist en volledig te zijn.
    - De vertrouwelijkheid dient te zijn gewaarborgd.
    - De communicatie dient zorgvuldig te verlopen.
3. Pensioendata
    - Bij aanpassing van systemen of conversie van data dienen rechten/aanspraken van deelnemers op de juiste en volledige wijze in stand te blijven. De rechten/aanspraken dienen reproduceerbaar te zijn.
4. Data beleggingsportefeuille
    - De juistheid en volledigheid van transacties dient altijd reproduceerbaar te zijn.
    - Door het niet beschikbaar zijn van systemen of verlies van data mag geen waarde en bezit verloren gaan nog de gegevens omtrent waarde en bezit.
5. Data inzake middelen op de bankrekening
    - De bescherming van waarden omvattende onder andere betaling voor legitieme diensten en legitieme uitkering van pensioengelden.
6. Besluitvorming en monitoring door bestuur
    - Juiste en tijdige besluitvorming door tijdige, juiste en volledige informatie.

7. De vijf grootste ICT-risico‘s

In vervolg op de beheers eisen heeft het bestuur vier ICT-risico‘s vastgesteld. Deze vier risico‘s sluiten aan bij het zogenaamde **4A** model[2]. Het bestuur vult deze 4 ICT risico ’s aan met bewustzijn.

1. Beschikbaarheid / (**A**vailabilty)
    - Het draaiend houden van bestaande processen en het herstellen van verstoringen, waarbij de negatieve gevolgen van incidenten zoals uitval en beveiligingslekken worden beperkt.
2. Toegang / (**A**ccess)
    - Het waarborgen dat de juiste mensen toegang hebben tot de juiste en volledige informatie en anderen niet.
3. Betrouwbaarheid / (**A**ccuracy)
    - Het opleveren van de juiste, tijdige en volledige informatie aan alle relevante partijen.
4. Aanpasbaarheid / (**A**gility)
    - Het ondersteunen van veranderingen in de bedrijfsvoering tegen acceptabele kosten en binnen acceptabele tijd.
5. Bewustzijn / (**A**wareness)
    - Het actief bevorderen van bewustzijn voor ICT-risico ‘s en voor cyberrisico’s bij medewerkers van het fonds en uitbestedingspartijen.

8. Eisen bij uitbesteding aan ICT- en informatievoorziening door het fonds

De volgende eisen bij uitbesteding aan ICT en dataverwerking worden door het fonds verlangd.
- Het fonds verlangt van haar uitvoeringspartijen een ISAE 3402 type 2 rapportage welke aantoont dat de uitbestede processen beheerst zijn. Zowel de financial als de ICT controls moeten beschreven zijn.
- De inrichting en realisatie van de benodigde ICT-middelen zijn overgedragen aan de uitvoeringspartijen. De afspraken over deze dienstverlening worden overeengekomen in een contract per uitvoeringspartij zodanig dat de uitbestede- en bedrijfsprocessen van het fonds gewaarborgd zijn.
- De uitvoeringspartijen hebben een eigen ICT-beleid mede gebaseerd op de door het fonds aan ICT verlangde eisen, de benoemde ICT- risico’s en gebaseerd op actuele marktconforme standaarden die voldoen aan wet- en regelgeving.
- Het fonds verlangt van de uitvoeringspartijen dat eventuele risico’s door middel van een risicoanalyse worden vertaald naar operationele maatregelen. Vanuit integraal risico management gezien verlangt het fonds dat de risico’s over de gehele uitbestede keten inzichtelijk zijn.
- De uitvoeringspartijen beschikken over risicomanagement beleid, informatiebeveiligings-, cybersecuritybeleid en business continuïteitsbeleid. De uitvoeringspartijen zijn verantwoordelijk voor het inrichten van de specifieke controls op basis waarvan de beheersing kan worden getoetst. Hierbij wordt rekening gehouden met de specifieke eisen vanuit wet- en regelgeving en toezichthouders. De wijze waarop het risicobeeld tot stand komt en de rapportage hierover aan het fonds wordt in onderling overleg bepaald waarbij het fonds zoveel mogelijk aansluit op de reguliere processen en rapportages vanuit de uitvoeringspartijen.
- Alle uitvoeringspartijen moeten voldoen aan de wet- en regelgeving die voortvloeit uit de Algemene Verordening Gegevensbescherming.
- Alle hiervoor verlangde eisen gelden ook voor de gehele keten/de sub uitvoeringspartijen van de genoemde hoofd uitvoeringspartijen.

[2] Het in de IT-wereld gebruikelijke 4A model is genoemd in het servicedocument ICT van de Pensioenfederatie, juli 2015

9. Monitoring ICT- en informatievoorzieningsbeleid bij uitvoeringspartijen

De contractuele afspraken die gemaakt zijn met de uitvoeringspartijen dienen beoordeeld te worden met betrekking tot het onderdeel ICT- en informatievoorziening. Vastgelegd dient te worden hoe de uitvoeringspartijen (laten) inventariseren, analyseren en rapporteren dat hun ICT en informatievoorziening voldoet aan door het fonds verlangde en de wettelijke gestelde eisen.
Met SLA 's en andere rapportages wordt aangetoond dat wordt voldaan aan de verlangde eisen uit deze beleidsnotitie. Periodiek stelt het bestuur van het fonds vast of de uitvoeringspartijen voldoen aan de verlangde beleidseisen. De beleggingsadvies- en dagelijks bestuur commissie bereiden deze vaststelling voor ten behoeve van het bestuur van het fonds.
In opdracht van het bestuur wordt per uitvoeringsorganisatie gecontroleerd of de gestelde ICT- en informatievoorzieningsbeleidseisen worden nageleefd hetgeen tenminste moet blijken uit SLA rapportages en ISAE-, en Cobit-rapportages.

10. Gestelde beleidseisen per aandachtsgebied

Hierna volgen de door het fonds verlangde eisen per aandachtsgebied om de ICT- en informatievoorzieningsbeleidseisen te realiseren. De aandachtsgebieden zijn Cloudcomputing, Informatiebeveiliging, Risicomanagement cyclus, Cybersecurity, Aanpasbaarheid en Beschikbaarheid.

10 a. Cloudcomputing

Cloudcomputing zorgt ervoor dat het lastiger wordt om aan te tonen dat aan de gevraagde beveiligingseisen is voldaan. Indien bij een uitvoeringspartij sprake is van Cloudcomputing past dit binnen de risicobereidheid van het bestuur. Een eis die wordt gesteld aan de uitvoeringspartijen is dat wanneer deze overgaan tot Cloudcomputing altijd eerst een risicoanalyse moet worden uitgevoerd. De uitvoeringspartijen dienen overgang naar of veranderingen omtrent Cloudcomputing vooraf te melden aan het fonds. Om de specifieke risico 's te beheersen rondom Cloudcomputing dienen de uitvoeringspartijen te beschikken over een actueel en geïmplementeerd Cloudbeleid en dit te communiceren met het fonds.

10 b. Informatiebeveiliging

Omdat het fonds en de uitvoeringspartijen een belangrijke maatschappelijke functie vervullen is het evident dat bij de verwerking van informatie rekening wordt gehouden met informatiebeveiliging. Het fonds stelt als eis dat alle uitvoeringspartijen qua inrichting en kaders rondom de beveiliging van informatie, minimaal moeten voldoen aan de AVG en de specifieke eisen van de toezichthouder DNB en Autoriteit Persoonsgegevens. Om de specifieke risico 's te beheersen rondom informatiebeveiliging dienen de uitvoeringspartijen te beschikken over een actueel en geïmplementeerd informatiebeveiligingsbeleid en dit te communiceren met het fonds.

In verband met het toezicht op naleving van de AVG wil het bestuur van het fonds dat de uitvoeringspartijen aansluiten bij goedgekeurde certificeringsmechanismes, bij voorkeur Cobit[3] of ISAE 3000 (assurance over niet financiële informatie) of bijvoorbeeld ISO 27000 (informatiebeveiligingsnormen).

[3] https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf, pagina 3, "In deze Good Practice is zoveel mogelijk aangesloten op de reeds bestaande indeling van de voorgaande 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek',1 maar is de directe link met Cobit losgelaten."

Daarmee tonen de uitvoeringspartijen aan dat wordt voldaan aan de AVG en de principes privacy by design en privacy by default. Privacy by design houdt in dat bij de verwerking gehanteerde mechanismen en systemen zo zijn ontworpen dat zoveel als mogelijk rekening wordt gehouden met de privacy van de deelnemers en de AVG. Privacy by default is het zodanig instellen van de standaardinstellingen dat de privacy zoveel als mogelijk wordt gewaarborgd.

Bij de informatievoorzieningsbeleid van het fonds zal rekening gehouden worden met de AVG. Het fonds beschikt over de bewijslast dat aan de AVG regelgeving wordt voldaan. Om aan te tonen dat aan de wetgeving wordt voldaan dienen alle risicovolle verwerkingen van persoonsgegevens onderworpen te worden aan een risicoanalyse. Een zogeheten Data Privacy Impact Assessment, afgekort DPIA. Ook zal het fonds een “verwerkingsregister” opstellen dat inzicht geeft in alle persoonsgegevens die door de organisatie en haar partners wordt beheerd. In het register moet onder andere inzicht worden gecreëerd welke persoonsgegevens het fonds verwerkt, welke verwerkingsdoeleinden er zijn, hoe lang de gegevens worden bewaard en welke maatregelen zijn getroffen om de privacyrisico’s te beperken. Verder heeft het fonds haar activiteiten en processen conform de AVG ingericht. Het fonds draagt zorgt voor documenteren, evalueren, wijzigen en verbeteren indien nodig. Het fonds besteedt aandacht aan de nieuwe rechten van betrokkenen, een Privacyverklaring op de website van het fonds, een functionaris voor gegevensbescherming, meldplicht datalekken, verwerkersovereenkomst met uitvoeringspartijen, garanties bij (onder-)uitbesteding, toestemming en profilering.

10 c. Risicomanagementcyclus

De risico’s die samenhangen met de verwerking van informatie worden opgenomen als onderdeel van de reguliere risicomanagementcyclus welke onderdeel is van het integraal risicomanagement. De cyclus kent de volgende fasen, identificeren, evalueren, beheersen en bewaken. Bij het fonds houdt de Risk-commissie zich bezig met het begeleiden en challengen van de 1e lijn, bestuur, beleggingsadviescommissie, communicatie commissie en dagelijks bestuur commissie die hiervoor primair verantwoordelijk is. De Risk-commissie rapporteert aan het bestuur.

Risicobereidheid

Het bestuur stelt de risicobereidheid voor het ICT-domein van het fonds vast. De uitvoeringspartijen zijn verantwoordelijk voor het vaststellen van hun risicobereidheid van de operationele risico ’s en sluiten aan bij de risicobereidheid van het fonds.

Identificatie en evaluatie

De uitvoeringspartijen zijn verantwoordelijk voor de uitvoering van een periodieke Business Impact Analyse. Deze analyse leidt tot een BIV score[4]. Een classificatie naar kwaliteitsaspecten Beschikbaarheid (B), Integriteit (I) en Vertrouwelijkheid (V). De BIV score vormt de input bij de periodieke risicoanalyse. Het resultaat van deze analyse is een overzicht van de belangrijkste risico ’s per proces bij de uitvoeringspartijen. Eventuele andere gereedschappen voor het identificeren en evalueren van risico ’s zijn, audit bevindingen, schade en incidenten analyses, risk en performance indicatoren, scenario analyses en analyse van het risicoprofiel van uitvoeringspartijen en deelname aan externe kennissessies.

[4] https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf, pag 30, 2.2 Data classification scheme

Beheersen
De uitvoeringsinstanties zijn verantwoordelijk dat de geïdentificeerde beheersmaatregelen zichtbaar worden geïmplementeerd in de bedrijfsprocessen. Van belang hierbij zijn de verlangde eisen van het fonds zoals beschreven, de toezichthouders, wet- en regelgeving en intern gehanteerde standaarden. Wanneer deze maatregelen niet of onvoldoende voorhanden zijn maken de uitvoeringspartijen een verbeterplan dat jaarlijks door de directie wordt vastgesteld. Voor het bestuur van het fonds werkt dit plan als stuur- en verantwoordingsdocument voor de inrichting van de risico mitigerende maatregelen.

Bewaken
De uitvoeringspartijen moeten periodiek een Risk Self Assessment op informatiebeveiliging uitvoeren. Daarbij kan gebruik worden gemaakt van de door DNB beschreven Good Practice Informatiebeveiliging[5]. Om de kwaliteit van deze controls te toetsen stellen de uitvoeringspartijen jaarlijks een testplan op. Hieruit komt een risicobeeld naar voren dat wordt aangevuld met incidenten en tussentijds uitgevoerde risico assessments. Afhankelijk van de risicobereidheid wordt bepaald of de risico 's aanleiding geven tot mitigerende acties.

Integraal risicomanagement
Het bestuur van het fonds eist een integraal risicomanagement over de gehele uitbestede ICT- en informatiebeveiligingsketen in te richten. De risicobeheersingsmaatregelen passend bij de BIV scores zoals toegekend aan de bedrijfskritische processen en daaraan gerelateerde informatiesystemen zoals applicaties, databases, infrastructuurcomponenten dienen hierbij aantoonbaar te zijn geïmplementeerd. Dit waarborgt dat de fondsdata adequaat zijn beveiligd tegen ongeautoriseerde wijzigingen, dat de data privacy voldoende gewaarborgd is en dat de data tijdig beschikbaar is voor de betrokken partijen bij het fonds.

10 d. Cybersecurity
Het fonds ziet cybersecurity als integraal onderdeel van informatiebeveiliging. Cybersecurity en de daarmee gepaard gaande risico 's hebben een hoge prioriteit, een lage risicobereidheid (risico willen lopen) en een lage risicotolerantie (risico kunnen lopen). Een eis is dat de uitvoeringspartijen zorgdragen voor een organisatie van de beveiliging die erop ingericht is de met cybersecurity gepaard gaande risico's te beheersen, tijdig te detecteren en de eventuele gevolgen van een incident te minimaliseren. De communicatiecommissie van het fonds draagt ook zorg voor het beperken van de impact van een incident door tijdige en duidelijke informatie. Periodiek wordt het fonds door de uitvoeringspartijen geïnformeerd over het gevoerde cybersecurity beleid en de beheersing van de cyberrisico's. Het fonds stelt verder als eis dat de uitvoeringspartijen voldoen aan de wet- en regelgeving op dit gebied alsmede de Good Practice Informatiebeveiling van DNB. Ook stelt het fonds als eis dat de uitvoeringspartijen tenminste voldoen aan de vier extra Cobit controls voor cybersecurity of maatregelen die vergelijkbaar werken.

[5] https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf

Deze vier beheersmaatregelen betreffen:

1. *Vulnerability management:*
   het actief monitoren en oplossen van kwetsbaarheden in de IT-infrastructuur van de instelling.
2. *Employee awareness:*
   het actief bevorderen van bewustzijn voor cyberrisico's bij medewerkers.
3. *Application Life cycle management:*
   borgen dat applicaties tijdig worden onderhouden en uitgefaseerd zodat het informatiebeveiligingsniveau niet in gevaar komt.
4. *Penetration testing and ethical hacking:*
   testen van de weerbaarheid tegen cyberrisico's.

Daarnaast wil het fonds geïnformeerd worden over welke persoon bij een uitvoeringorganisatie de privacybeschermer, de ketenregisseur en de incidentenmanager voor het fonds is.

10 e. Aanpasbaarheid

Het fonds stelt als eis dat de uitvoeringspartijen hun producten en diensten beschikbaar stellen afgestemd op de specifieke behoefte van het fonds tegen een zo laag mogelijke investering en jaarlijkse kosten. De uitvoeringspartijen realiseren deze eis met inzet van geautomatiseerde systemen, waarin standaardisatie en klantdifferentiatie in onderling evenwicht zijn geoptimaliseerd. Dit houdt in harmonisatie van processen en standaardisatie van systemen. Een harde eis voor alle uitvoeringspartijen is dat ICT is aangelijnd aan de "business". Dit houdt in dat ICT-specialisten samenwerken met pensioendeskundigen, beleggingsdeskundigen. Verder eist het fonds dat projectdoelen tijdig gehaald worden en dat de bestaande ICT toekomstbestendig is. De ICT dient een aanpassing van de pensioenwetgeving, een mogelijke overgang van collectief naar meer individueel aan te kunnen. De uitvoeringspartijen dienen te onderbouwen waarom hun systemen toekomst bestendig zijn. Deze onderbouwing dienen zij te rapporteren aan het fonds.

10 f. Beschikbaarheid

De uitvoeringspartijen bieden producten en diensten met een overeengekomen stabiliteit van de bedrijfsvoering op het gebied van vermogensbeheer, pensioenbeheer en ICT voor het bestuur en bureau pensioenzaken. De uitvoeringspartijen zijn voorbereid op eventuele calamiteiten die de dienstverlening kunnen raken in de vorm van een Business Continuity Management Beleid en aantoonbare werking daarvan. Een onderdeel hiervan is minimaal een jaarlijkse crisismanagement oefening en ICT-uitwijktest. De uitvoeringspartijen hanteren een locatieonafhankelijke werkwijze met bijbehorende methoden en technieken. De bedrijfsinrichting en het ontwerp van de informatievoorziening wordt gekenmerkt door een aanpak, waarbij waar nodig, schaalbare oplossingen worden ingezet, gebaseerd op marktstandaarden. Als randvoorwaarde voor operationele stabiliteit geldt dat hard- en software verregaand is gestandaardiseerd en risicogedreven wordt beheerd.

10g. Versiebeheer

Versie	Wijzigingen Bijzonderheden	Auteur	Datum vaststellen
Versie 1 Beleidsnotitie ICT en informatievoorziening 2018-2020	Initiële vastlegging ICT en informatievoorziening beleid	Werkgroep ICT De heer Mulders De heer Tijhuis De heer Heemskerk De heer Harperink	Bestuur 19-1-2018
Versie 2 Beleidsnotitie ICT en informatievoorziening 2021-2023	Algehele update beleid. De 54-Cobit controls van DNB zijn uitgebreid naar 58-Cobit controls. Deze uitbreiding van de controls ziet op cybercrime.	De heer Harperink Review de heer Heemskerk	Bestuur 6-11-2020
Versie 3 Beleidsnotitie ICT, informatievoorziening en cybersecurity 2023-2025	Algehele update beleid. Beleid in lijn brengen met de Good Practice IB 2019-2020 van DNB. Naam uitbreiden met cybersecurity.	De heer Harperink Review de heer Heemskerk	Bestuur 22-9-2023